Приказ Министерства образования и науки РФ от 17 января 2011 г. N 50 "Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки (специальности) 090302 Информационная безопасность телекоммуникационных систем (квалификация (степень) "специалист")"

В соответствии с пунктом 5.2.7 Положения о Министерстве образования и науки Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 15 мая 2010 г. N 337 (Собрание законодательства Российской Федерации, 2010, N 21, ст. 2603; N 26, ст. 3350), пунктом 7 Правил разработки и утверждения федеральных государственных образовательных стандартов, утвержденных постановлением Правительства Российской Федерации от 24 февраля 2009 г. N 142 (Собрание законодательства Российской Федерации, 2009, N 9, ст. 1110), приказываю:

Утвердить прилагаемый федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки (специальности) 090302 Информационная безопасность телекоммуникационных систем (квалификация (степень) "специалист") и ввести его в действие со дня вступления в силу настоящего приказа.

Министр А.А. Фурсенко

Зарегистрировано в Минюсте РФ 31 марта 2011 г.
Регистрационный N 20352

Приложение

Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки (специальности) 090302 Информационная безопасность телекоммуникационных систем (квалификация (степень) "специалист") (утв. приказом Министерства образования и науки РФ от 17 января 2011 г. N 50)

Комментарий ГАРАНТа

См. справку о федеральных государственных образовательных стандартах

I. Область применения

1.1. Настоящий федеральный государственный образовательный стандарт высшего профессионального образования (ФГОС ВПО) представляет собой совокупность требований, обязательных при реализации основных образовательных программ подготовки специалистов по направлению подготовки (специальности) 090302 Информационная безопасность телекоммуникационных систем образовательными учреждениями высшего профессионального образования (высшими учебными заведениями, вузами), имеющими государственную аккредитацию, на территории Российской Федерации.

1.2. Право на реализацию основных образовательных программ высшее учебное заведение имеет только при наличии соответствующей лицензии, выданной уполномоченным федеральным органом исполнительной власти.

II. Используемые сокращения

В настоящем стандарте используются следующие сокращения:

ВПО	- высшее профессиональное образование;
ООП	- основная образовательная программа;
ОК	- общекультурные компетенции;
ПК	- профессиональные компетенции;
ПСК	- профессионально-специализированные компетенции;
УЦ ООП	- учебный цикл основной образовательной программы;
ФГОС ВПО	- федеральный государственный образовательный стандарт высшего профессионального образования.

III. Характеристика направления подготовки (специальности)

Нормативный срок, общая трудоемкость освоения ООП (в зачетных единицах)* и соответствующая квалификация (степень) приведены в таблице 1.

Таблица 1

Сроки, трудоемкость освоения ООП и квалификация (степень) выпускников

Наименование ООП	Квалификация (степень)		Нормативный срок освоения ООП (для очной формы обучения), включая каникулы, предоставляемые после прохождения итоговой государственной аттестации	Трудоемкость (в зачетных единицах)
	Код в соответствии с принятой классификацией ООП	Наименование		
ООП подготовки специалиста	65	специалист	5,5 лет	330*

_____

* Трудоемкость основной образовательной программы подготовки специалиста по очной форме обучения в среднем за учебный год равна 60 зачетным единицам.

По данной ООП подготовки специалиста обучение в форме очно-заочной (вечерней), заочной и экстерната не допускается.

IV. Характеристика профессиональной деятельности специалистов

4.1. Область профессиональной деятельности специалистов включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с проектированием, созданием, исследованием и эксплуатацией систем обеспечения информационной безопасности телекоммуникационных систем в условиях существования угроз в информационной сфере.

4.2. Объектами профессиональной деятельности специалистов являются: методы, средства и системы обеспечения информационной безопасности информационно-телекоммуникационных сетей и систем; управление информационной безопасностью информационно-телекоммуникационных сетей и систем; информационно-телекоммуникационные сети и системы различного назначения, их оборудование, принципы построения.

4.3. Специалист по направлению подготовки (специальности) 090302 Информационная безопасность телекоммуникационных систем готовится к следующим видам профессиональной деятельности:

научно-исследовательская;

проектная;

контрольно-аналитическая;

организационно-управленческая;

эксплуатационная.

Конкретные виды профессиональной деятельности, к которым в основном готовится специалист, определяются высшим учебным заведением совместно с обучающимися, научно-педагогическими работниками высшего учебного заведения и объединениями работодателей.

По окончании обучения по направлению подготовки (специальности) 090302 Информационная безопасность телекоммуникационных систем, наряду с квалификацией (степенью) "специалист" присваивается специальное звание "специалист по защите информации".

4.4. Специалист по направлению подготовки (специальности) 090302 Информационная безопасность телекоммуникационных систем должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

научно-исследовательская деятельность:

сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности телекоммуникационных систем, выработка предложений по вопросам комплексного обеспечения информационной безопасности таких систем;

подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;

изучение, анализ и обобщение опыта работы учреждений, организаций и предприятий по использованию технических средств и способов защиты информации в телекоммуникационных системах с целью повышения эффективности и совершенствования работ по ее защите;

сопровождение разработки, исследование технических и программно-аппаратных средств защиты и обработки информации в телекоммуникационных системах;

разработка моделей угроз информационной безопасности телекоммуникационных систем;

исследование защищенных сетей и систем передачи информации;

определение требований по защите информации, анализ защищенности телекоммуникационных систем и оценка рисков нарушения их информационной безопасности;

проектная деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации;

сравнительный анализ сетей и систем передачи информации по показателям информационной безопасности;

разработка проектов, технических заданий, планов и графиков проведения работ по защите информации телекоммуникационных систем и необходимой технической документации;

рациональный выбор элементной базы при проектировании устройств и систем защиты информации телекоммуникационных систем;

разработка политики безопасности, выбор методов и средств обеспечения информационной безопасности объектов информационно-телекоммуникационных систем;

проектирование защищенных информационно-телекоммуникационных систем;

оценка соответствия результатов проектирования требованиям технического задания;

контрольно-аналитическая деятельность:

проверка работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

инструментальный мониторинг защищенности телекоммуникационных систем;

выполнение технических работ при аттестации телекоммуникационных систем с учетом требований по защите информации;

проверка учреждений, организаций и предприятий на соответствие требованиям нормативной и правовой базы в области информационной безопасности телекоммуникационных систем;

подготовка отзывов и заключений на нормативно-методические материалы и техническую документацию;

участие в проведении аттестации телекоммуникационных систем, технических средств на предмет соответствия требованиям защиты информации по соответствующим классам безопасности;

организационно-управленческая деятельность:

организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;

разработка предложений по совершенствованию и повышению эффективности принимаемых технических мер и организационных мероприятий;

организация работ по выполнению требований режима защиты информации ограниченного доступа;

разработка методических материалов и организационно-распорядительных документов по обеспечению информационной безопасности телекоммуникационных систем на предприятиях отрасли;

эксплуатационная деятельность:

эксплуатация специальных технических и программно-аппаратных средств защищенных телекоммуникационных сетей и систем;

документационное обеспечение эксплуатации защищенных телекоммуникационных сетей и систем;

составление методик расчетов и программ экспериментальных исследований по защите информации телекоммуникационных систем, выполнение расчетов в

соответствии с разработанными методиками и программами;

выявление возможных источников и технических каналов утечки информации;

определение технических характеристик сетей передачи информации общего и специального назначения;

обеспечение восстановления работоспособности систем защиты информации при сбоях и нарушении функционирования.

V. Требования к результатам освоения основных образовательных программ подготовки специалиста

5.1. Выпускник должен обладать следующими общекультурными компетенциями (ОК):

способностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (ОК-1);

способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики (ОК-2);

способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач (ОК-3);

способностью понимать движущие силы и закономерности исторического процесса, роль личности в истории, политической организации общества, способностью уважительно и бережно относиться к историческому наследию, толерантно воспринимать социальные и культурные различия (ОК-4);

способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и зашиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-5);

способностью к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (ОК-6);

способностью логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

способностью к письменной и устной деловой коммуникации, к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков (ОК-8);

способностью к логически-правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания (ОК-9);

способностью самостоятельно применять методы и средства познания,

обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой деятельности, развития социальных и профессиональных компетенций, изменения вида своей профессиональной деятельности (ОК-10);

способностью к осуществлению воспитательной и образовательной деятельности (ОК-11);

способностью самостоятельно применять методы физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, достижения должного уровня физической подготовленности в целях обеспечения полноценной социальной и профессиональной деятельности (ОК-12).

5.2. Выпускник должен обладать следующими профессиональными компетенциями (ПК):

общепрофессиональными:

способностью выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения (ПК-1);

способностью применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2);

способностью понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-3);

способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-4);

способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);

способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК-6);

способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ПК-7);

способностью определять погрешности вычислений и применять стандартные пакеты численных вычислений (ПК-8);

способностью к эксплуатации современного телекоммуникационного оборудования и приборов (ПК-9);

способностью применять основные методы, способы и средства получения, хранения, переработки и передачи информации (ПК-10);

в научно-исследовательской деятельности:

способностью осуществлять подбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-11);

способностью применять современные методы исследования с использованием компьютерной техники (ПК-12);

способностью проводить математическое моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований (ПК-13);

способностью выявлять тенденции развития информационной безопасности

телекоммуникационных систем (ПК-14);

способностью формулировать задачи и проводить исследования телекоммуникационных систем и оценивать их эффективность (ПК-15);

способностью планировать и проводить экспериментальное исследование телекоммуникационных систем (ПК-16);

способностью оценивать технические возможности и вырабатывать рекомендации по построению систем и сетей передачи информации общего и специального назначения (ПК-17);

в проектной деятельности:

способностью участвовать в разработке компонентов телекоммуникационных систем (ПК-18);

способностью проектировать защищенные телекоммуникационные системы и проводить анализ проектных решений по обеспечению безопасности телекоммуникационных систем (ПК-19);

способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-20);

способностью прогнозировать, ранжировать, моделировать информационные угрозы телекоммуникационных систем и оценивать уровни риска (ПК-21);

способностью осуществлять рациональный выбор элементной базы обеспечения информационной безопасности телекоммуникационных систем и их устройств (ПК-22);

в контрольно-аналитической деятельности:

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации телекоммуникационных систем с учетом нормативных требований по защите информации (ПК-23);

способностью оценивать эффективность систем защиты информации в телекоммуникационных системах (ПК-24);

способностью осуществлять аудит уровня защищенности и аттестацию телекоммуникационных систем (ПК-25);

способностью оценивать степень выполнения требований нормативных правовых актов и нормативных методических документов в области информационной безопасности и подготовки соответствующих заключений (ПК-26);

в организационно-управленческой деятельности:

способностью разрабатывать планы работы первичных подразделений и организовывать их выполнение в условиях спектра мнений (ПК-27);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы (ПК-28);

способностью организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности (ПК-29);

способностью оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности (ПК-30);

способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-31);

в эксплуатационной деятельности:

способностью эксплуатировать системы и средства обеспечения информационной безопасности телекоммуникационных систем (ПК-32);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов телекоммуникационных систем (ПК-33);

способностью определять технические характеристики телекоммуникационных систем (ПК-34);

способностью проводить мониторинг, техническую диагностику средств защиты и оценку эффективности информационной безопасности защищенных телекоммуникационных систем (ПК-35).

Специализация N 1 "Мониторинг в телекоммуникационных системах".

Специализация N 2 "Системы представительской связи".

В соответствии с пунктом 7.1 настоящего стандарта требования к специализации определяются вузом

Специализация N 3 "Сети специальной связи".

Специализация N 4 "Инструментальный контроль информационной безопасности телекоммуникационных систем".

Специализация N 5 "Системы специальной связи и информации для органов государственной власти".

Специализация N 6 "Информационная безопасность космических телекоммуникационных систем":

способностью осваивать современные перспективные направления развития телекоммуникационных космических и наземных систем радиосвязи и навигации (ПСК-6.1);

способностью реализовывать новые принципы построения защищенных космических телекоммуникационных систем (ПСК-6.2);

способностью разрабатывать средства и методы защиты информации в системах космической радиосвязи и навигации (ПСК-6.3);

способностью разрабатывать модели защищенного телеуправления космическими аппаратами и их проверки на практике (ПСК-6.4);

способностью эксплуатировать защищенные системы спутниковой радиосвязи и навигации (ПСК-6.5);

Специализация N 7 "Разработка защищенных телекоммуникационных систем":

способностью разрабатывать алгоритмы преобразования информации и сигналов для защищенных телекоммуникационных систем на основе теоретико-числовых методов (ПСК-7.1);

способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных телекоммуникационных система (ПСК-7.2);

способностью разрабатывать аппаратное и программное обеспечение узлов и устройств защищенных телекоммуникационных систем на базе сигнальных процессоров (ПСК-7.3);

способностью участвовать в разработке и оценке соответствия средств защиты информации подсистем обеспечения информационной безопасности защищенных телекоммуникационных систем требованиям по безопасности информации (ПСК-7.4);

способностью участвовать в разработке систем менеджмента информационной безопасности телекоммуникаций (ПСК-7.5);

способностью планировать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности телекоммуникаций (ПСК-7.6);

способностью обеспечивать защиту программных средств защищенных телекоммуникационных систем (ПСК-7.7);

Специализация N 8 "Системы подвижной цифровой защищенной связи":

способностью использовать и реализовывать алгоритмы обработки информации

и сигналов в подвижных цифровых защищенных телекоммуникационных системах связи (ПСК-8.1);

способностью понимать и использовать принципы работы и методы эксплуатации систем подвижной цифровой защищенной связи (ПСК-8.2);

способностью выбирать методы и разрабатывать алгоритмы принятия решений для обеспечения безопасности систем подвижной цифровой защищенной связи (ПСК-8.3);

способностью модифицировать аппаратное и программное обеспечение узлов и устройств систем подвижной цифровой защищенной связи (ПСК-8.4);

способностью готовить документацию на проведение научно-исследовательской работы по разработке подсистем обеспечения информационной безопасности подвижной цифровой защищенной связи (смет, заявок на материалы, оборудование, трудовых договоров) (ПСК-8.5);

способностью разрабатывать документационное обеспечение функционирования подсистем подвижной цифровой защищенной связи (ПСК-8.6);

Специализация N 9 "Защита информации в радиосвязи и телерадиовещании":

способностью разрабатывать системы, средства и методы защиты информации в сетях, системах и устройствах радиосвязи и телерадиовещания (ПСК-9.1);

способностью использовать нормативно-правовые акты и нормативные методические документы в области технологий и систем радиосвязи и телерадиовещания (ПСК-9.2);

способностью участвовать в работе по межотраслевой координации и взаимодействию операторов в области электросвязи в части технологий радиодоступа и организации массового оповещения населения в чрезвычайных ситуациях (ПСК-9.3);

способностью участвовать в процедурах назначения, распределения и эффективного использования радиочастотного спектра (ПСК-9.4);

способностью проводить монтаж и эксплуатацию технических средств радиосвязи и телерадиовещания (ПСК-9.5);

способностью применять методы повышения помехоустойчивости и защищённости систем радиосвязи и телерадиовещания и определять области наиболее эффективного их использования (ПСК-9.6);

способностью проводить инструментальные измерения основных характеристик и параметров телекоммуникационных систем (ПСК-9.7);

способностью организовывать и проводить испытания средств защищенной радиосвязи и телерадиовещания с целью оценки их соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов (ПСК-9.8);

Специализация N 10 "Защита информации в системах связи и управления":

способностью анализировать основные информационные процессы в системах связи и управления и выделять основные задачи обеспечения безопасности информации в компьютерных и телекоммуникационных системах (ПСК-10.1);

способностью применять теорию сигналов и систем для анализа телекоммуникационных систем и оценки их помехоустойчивости (ПСК-10.2);

способностью формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем (ПСК-10.3);

способностью оценивать возможности средств технических разведок в отношении к системам связи и управления (ПСК-10.4);

способностью применять наиболее эффективные методы и средства для

закрытия возможных каналов перехвата акустической речевой информации (ПСК-10.5);

способностью обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи (ПСК-10.6);

способностью проводить инструментальную оценку уровня защищенности информационно-телекоммуникационных систем и объектов информатизации (ПСК-10.7);

Специализация N 11 "Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте":

способностью проводить теоретические и экспериментальные исследования интегрированных телекоммуникационных систем, цифровых сетей технологической связи и беспроводного доступа и корпоративных сетей транспорта (по видам) и оценивать их эффективность (ПСК-11.1);

способностью осуществлять рациональный выбор методов и средств обеспечения информационной безопасности телекоммуникационных систем и корпоративных сетей транспорта (по видам) (ПСК-11.2);

способностью разрабатывать предложения по совершенствованию системы аудита и управления информационной безопасностью телекоммуникационной системы транспорта (по видам) (ПСК-11.3);

способностью к профессиональной эксплуатации современного оборудования и приборов, использовать методы и средства измерений для решения метрологических задач и технической диагностики защищенных сетей транспорта (по видам) (ПСК-11.4);

способностью обеспечить эффективную защиту цифровых сетей технологической связи и беспроводного доступа и корпоративных сетей транспорта (по видам) (ПСК-11.5).

Специализация N 12 "Безопасность телекоммуникационных систем информационного взаимодействия":

способностью выполнять декомпозицию сложных информационных систем, формулировать показатели их эффективности с целью построения корректной концептуальной модели систем (ПСК-12.1);

способностью обоснованно выбирать и (или) строить адекватные, математические и алгоритмические модели, в том числе с помощью высокоуровневых средств, для эффективного проектирования телекоммуникационных систем информационного взаимодействия (ПСК-12.2);

способностью обоснованно выбирать конкурентно-способные программные технологии для реализации компонентов телекоммуникационных систем информационного взаимодействия, выполнять сравнительную оценку их эффективности (ПСК-12.3);

способностью обоснованно выбирать и применять адекватные методы кодирования для построения высокоэффективных телекоммуникационных систем информационного взаимодействия и систем управления их поведением (ПСК-12.4);

способностью обоснованно выбирать и применять базовые криптографические алгоритмы и технологии для защиты данных в процессе информационного взаимодействия и осуществления управляющих актов в телекоммуникационных системах информационного взаимодействия (ПСК-12.5);

способностью обоснованно выбирать конкурентно-способные варианты организации многоуровневых клиент-серверных сетевых архитектур телекоммуникационных систем информационного взаимодействия, оптимизировать информационные потоки, загрузку узлов и требования к их безопасности (ПСК-12.6);

способностью проводить сравнительную оценку угроз при передаче различных

видов информации и предлагать систему мер для их предотвращения (ПСК-12.7);

способностью анализировать информационные потоки на пакетном уровне, оценивать реальный уровень безопасности информационного взаимодействия и предлагать эффективные меры для его повышения (ПСК-12.8);

способностью применять стандартные средства для анализа программного кода с целью оценки уровня его защиты от исследования и поиска несанкционированного или вредоносного вмешательства в работу телекоммуникационных систем информационного взаимодействия (ПСК-12.9).

VI. Требования к структуре основных образовательных программ подготовки специалиста

6.1. ООП подготовки специалиста предусматривает изучение следующих учебных циклов (таблица 2):

гуманитарный, социальный и экономический циклы;

математический и естественнонаучный цикл;

профессиональный цикл;

и разделов:

физическая культура;

учебная и производственная практики, научно-исследовательская работа;

итоговая государственная аттестация.

6.2. Каждый учебный цикл имеет базовую (обязательную) часть и вариативную, устанавливаемую вузом. Вариативная часть дает возможность расширения и (или) углубления знаний, умений и навыков, определяемых содержанием базовых (обязательных) дисциплин (модулей) и дисциплин специализаций, позволяет обучающемуся получить углубленные знания и навыки для успешной профессиональной деятельности и (или) для продолжения профессионального образования в аспирантуре (адъюнктуре).

6.3. Базовая (обязательная) часть цикла "Гуманитарный, социальный и экономический цикл" должна предусматривать изучение следующих обязательных дисциплин: "История Отечества", "Философия", "Иностранный язык".

Базовая (обязательная) часть профессионального цикла должна предусматривать изучение всех дисциплин, определенных структурой ООП подготовки специалиста.

Таблица 2

Структура ООП подготовки специалиста

Код УЦ ООП	Учебные циклы (разделы) и проектируемые результаты их освоения	Трудоемкость (Зачетные единицы)*	Перечень дисциплин для разработки программ (примерных), а также учебников и учебных пособий	Коды формируемых компетенций
С.1	Гуманитарный, социальный и экономический цикл	32-39		

	Базовая часть В результате изучения базовой части цикла студент должен: знать: - содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных, социальных и экономических наук; - основные этапы развития философской мысли, основную проблематику и структуру философского знания; - основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; - лексический и грамматический минимум в объеме, необходимом для работы с текстами профессиональной направленности и осуществления коммуникации на иностранном языке; - основные экономические теории, категории и закономерности, методы анализа экономических явлений и процессов; - основы экономической и финансовой деятельности отрасли и ее структурных подразделений, методику оценки хозяйственной, деятельности (применительно к отрасли обеспечения информационной безопасности); - основы права и законодательства России, основы конституционного	22-29***	Философия История Отечества Иностранный язык Экономика Правоведение Основы управленческой деятельности	ОК-1 ОК-2 ОК-3 ОК-4 ОК-5 ОК-6 ОК-7 ОК-8 ОК-9 ОК-10 ОК-11 ПК-5 ПК-6 ПК-18 ПК-27 ПК-29 ПК-30 ПК-31

	строя Российской Федерации, характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации; - научные основы, цели, принципы, методы и технологии управленческой деятельности; уметь: - использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач; - анализировать мировоззренческие, социально и личностно значимые философские проблемы; - анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности; - читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи; - анализировать экономические показатели деятельности подразделения; - использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой			

	в профессиональной деятельности; - уметь работать в коллективе, принимать управленческие решения и оценивать их эффективность; владеть: - основными методами научного познания; - иностранным языком в объеме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке; - навыками письменного аргументированного изложения собственной точки зрения; - навыками публичной речи, аргументации, ведения дискуссии и полемики; - навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками выбора, обоснования, реализации и контроля результатов управленческого решения.			
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	8-10		
С.2	Математический и естественнонаучный цикл	74-84		
	Базовая часть В результате изучения базовой части цикла обучающийся должен: знать: - основные понятия и задачи векторной алгебры и аналитической геометрии; - основные свойства алгебраических структур; - основные положения	66-72***	Математический анализ Алгебра и геометрия Теория вероятностей и математическая статистика Дискретная математика Теория	ОК-5 ОК-7 ОК-8 ОК-9 ОК-10 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-7

	теории пределов функций, теории рядов; - основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных; - основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики; - основные понятия и методы дискретной математики; - основные понятия теории информации и кодирования: энтропия, взаимная информация, источники сообщений, каналы связи, коды; - основные результаты о кодировании при наличии и отсутствии шума; - основные понятия оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи; - основные законы механики; - основные законы термодинамики и молекулярной физики; - основные законы электричества и магнетизма; основы теории колебаний и волн, оптики; - основы квантовой физики и физики твёрдого тела; - физические явления и эффекты, используемые при обеспечении информационной безопасности телекоммуникационных систем; - основные понятия информатики;		информации и кодирования Физика Информатика Языки программирования	ПК-8 ПК-9 ПК-10

	- формы и способы представления данных в персональном компьютере; - состав и назначение функциональных компонентов и программного обеспечения персонального компьютера; - классификацию современных компьютерных систем; - типовые структуры и принципы организации компьютерных сетей; - области и особенности применения языков программирования высокого уровня; - язык программирования высокого уровня (объектно-ориентированное программирование); уметь: - строить и изучать математические модели для решения расчетных и исследовательских задач; - определять возможности применения методов математического анализа; - решать основные задачи векторной алгебры и аналитической геометрии; - решать основные задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды; - решать основные задачи линейной алгебры, системы линейных уравнений над полями; - оперировать в числовых и конечных полях, с многочленами и матрицами; - применять стандартные методы и модели к			

	решению теоретико-вероятностных и статистических задач в профессиональной области; - пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач; - применять методы дискретной математики для решения профессиональных задач; - вычислять теоретико-информационные характеристики источников сообщений и каналов связи; - строить математические модели физических явлений и процессов; - решать типовые прикладные физические задачи; - анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; - применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); - пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; - работать с интегрированной средой разработки программного обеспечения; - реализовывать на языке высокого уровня алгоритмы			

	решения профессиональных задач, в том числе задач обработки битовых потоков; владеть: - навыками использования методов математического анализа к решению прикладных задач; - навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; - методами линейной алгебры; - навыками использования теоретико-вероятностных и статистических методов при решении прикладных - навыками построения дискретных моделей при решении профессиональных задач; - основами построения математических моделей систем передачи информации; - навыками применения математического аппарата для решения прикладных теоретико-информационных задач; - навыками пользования библиотеками прикладных программ для решения прикладных математических задач; - методами теоретического исследования физических явлений и процессов; - навыками проведения физического эксперимента и обработки его результатов; - навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки			

	презентационных материалов); - навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов); - навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); - навыками разработки, документирования, тестирования и отладки программ.			
	1. Специализация "Мониторинг в телекоммуникационных системах"**	6-9		
	2. Специализация "Системы представительской связи"**	6-9		
	3. Специализация "Сети специальной связи"**	6-9		
	4. Специализация "Инструментальный контроль информационной безопасности телекоммуникационных систем"**	6-9		
	5. Специализация "Системы специальной связи и информации для органов государственной власти"**	6-9		
	6. Специализация "Информационная безопасность космических телекоммуникационных систем" С целью получения данной специализации при изучения базовой части цикла обучающийся	6-9	Математические методы теории сигналов и систем	ПСК-6.1 ПСК-6.2

	должен: знать: - свойства преобразования Лапласа, дискретного и непрерывного преобразований Фурье, Z-преобразования, вейвлет-анализа; уметь: - использовать математические модели сигналов при решении задач передачи информации; владеть: - навыками применения математического аппарата к анализу непрерывных, дискретных и цифровых сигналов и систем			
	7. Специализация "Разработка защищенных телекоммуникационных систем" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - основные понятия и теоремы теории чисел, основные свойства групп, колец, полей; - принципы построения ортонормированных конечномерных базисов; - основные понятия теории конфликтов, теории принятия решений; уметь: - решать прикладные задачи теории чисел и модулярной арифметики; - выбирать методы и модели принятия решений в защищенных автоматизированных системах управления; владеть:	6-9	Основы теории чисел Теория принятия решений в условиях информационных конфликтов	ПСК-7.1 ПСК-7.2

	- навыками решения прикладных задач с применением групп, колец и полей; - навыками выбора и оптимизации вида базисных функций, соответствующих обрабатываемым сигналам и элементной базе; - навыками разработки алгоритмов защиты от принятия несвоевременных и ложных решений; - навыками оценки вычислительной сложности реализации выбранных или разработанных алгоритмов принятия решений.			
	8. Специализация "Системы подвижной цифровой защищенной связи" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - основные понятия и алгоритмы численного поиска экстремумов функций, решения линейных и нелинейных алгебраических уравнений и решения дифференциальных и интегральных уравнений; уметь: - оценивать погрешности вычислений и применять методы оценки сложности и устойчивости алгоритмов; владеть: - численными методами решения задач линейной и нелинейной алгебры, решения экстремальных задач и численного интегрирования, решения	6-9	Методы математического моделирования	ПСК-8.1

дифференциальных и интегральных уравнений.			
9. Специализация "Защита информации в радиосвязи и телерадиовещании" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - основы математического аппарата, применяемого для решения задач теории массового обслуживания и телетрафика, повышения помехоустостойчивости радиосвязи; уметь: - использовать математические методы теории массового обслуживания и телетрафика, статистические методы помехозащищённой радиосвязи, методы устранения избыточности и кодирования звуковых и видео сигналов в конкретных технических приложениях; - строить вероятностные модели для исследуемых процессов, проводить необходимые расчеты в рамках построенной модели; владеть: - методами аналитического и численного решения статистических задач радиосвязи.	6-9	Основы теории массового обслуживания Теоретические основы помехоустойчивой радиосвязи	ПСК-9.6 ПСК-9.7
10. Специализация "Защита информации в системах связи и управления" С целью получения данной специализации при изучении базовой части	6-9	Введение в специальность Математические методы теории сигналов и систем	ПСК-10.1 ПСК-10.2

	цикла обучающийся должен: знать: - основные информационные процессы в системах связи и управления; - основные задачи обеспечения безопасности информации в компьютерных и телекоммуникационных системах; - свойства преобразования Лапласа, дискретного и непрерывного преобразований Фурье, Z-преобразования, вейвлет-анализа; уметь: - использовать математические модели сигналов при решении задач передачи информации; владеть: - навыками применения математического аппарата к анализу непрерывных дискретных и цифровых сигналов и систем.			
	11. Специализация "Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - конструкцию и стандарты оптических волокон и кабелей, виды затухания оптических волокон, рабочие длины волн оптических волокон;	6-9	Волоконнооптические направляющие системы	ПСК-11.1 ПСК-11.2 ПСК-11.3 ПСК-11.4 ПСК-11.5

	- особенности распространения излучения в волоконнооптических направляющих системах, влияние на распространение излучения различных неоднородностей и электромагнитного излучения; принципы оптических измерений; уметь: - рассчитывать основные характеристики волоконнооптических направляющих систем; - выбирать рабочие длины волн, тип и конструкцию волоконнооптического кабеля для телекоммуникационных систем; владеть: - навыками расчета характеристик в волоконнооптических направляющих системах, разделки волоконнооптического кабеля. 12. Специализация "Безопасность телекоммуникационных систем информационного взаимодействия" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - назначение систем информационного взаимодействия; - основные информационные процессы в системах информационного взаимодействия; - основные задачи			

	обеспечения безопасности систем информационного взаимодействия; - основы теории чисел и алгебры полей Галуа; уметь: - строить числовые и алгебраические модели кодирующих преобразований; - формулировать задачу кодирующих преобразований в терминах линейных переключающих схем; владеть: - аппаратом теории чисел и алгебры полей Галуа для представления кодирующих преобразований, анализа их сложности и оценки основных показателей эффективности.			
		6-9	Прикладные вопросы дискретной математики Введение в специальность	ПСК-12.1 ПСК-12.2 ПСК-12.4 ПСК-12.5
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	8-12		
С.3	Профессиональный цикл	160-170		
	Базовая часть В результате изучения базовой части цикла обучающийся должен: знать: - сущность и понятие информации, информационной безопасности и характеристику ее составляющих; - место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной	110-116***	Основы информационной безопасности Организационное и правовое обеспечение информационной безопасности Техническая защита информации Безопасность жизнедеятельности Электроника и схемотехника Сети и системы	ОК-1 ОК-2 ОК-5 ОК-6 ОК-7 ОК-8 ОК-9 ОК-10 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9

	информационной политики, стратегию развития информационного общества в России; - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; - основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; организацию работы и нормативные правовые акты и стандарты по - лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; - технические каналы утечки информации;		передачи информации Методы программирования Информационные технологии Криптографические методы защиты информации Программно-аппаратные средства обеспечения информационной безопасности Теория электрических цепей Теория радиотехнических сигналов Антенны и распространение радиоволн Теория электрической связи Квантовая и оптическая электроника Аппаратные средства телекоммуникационных систем Цифровая обработка сигналов Инженерная графика Измерения в телекоммуникационных системах Проектирование защищенных телекоммуникационных систем Информационная безопасность телекоммуникационных систем	ПК-10 ПК-11 ПК-12 ПК-13 ПК-14 ПК-15 ПК-16 ПК-17 ПК-18 ПК-19 ПК-20 ПК-21 ПК-22 ПК-23 ПК-24 ПК-25 ПК-26 ПК-27 ПК-28 ПК-29 ПК-30 ПК-31 ПК-32 ПК-33 ПК-34 ПК-35

	- возможности технических средств перехвата информации; - способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - организацию защиты информации от утечки по техническим каналам на объектах информатизации; - основы физической защиты объектов информатизации; - опасные и вредные факторы системы "человек - среда обитания", - научные и организационные основы защиты окружающей среды и ликвидации последствий, аварий, катастроф, стихийных бедствий; - принципы работы элементов и функциональных узлов электронной аппаратуры; - методы анализа и синтеза электронных схем; - типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; - основы построения систем и сетей электросвязи включая мультисервисные сети связи; - эталонную модель взаимодействия открытых систем; - современные виды информационного взаимодействия и обслуживания; - представление информации в телекоммуникационных системах и методы ее		Моделирование систем и сетей телекоммуникаций	

	обработки; - основные стандарты, протоколы и интерфейсы, используемые в телекоммуникационных системах; - перспективные направления развития телекоммуникационных систем; - назначение, функции и структуру операционной системы; - назначение и основные компоненты систем баз данных; - основы построения и структуру информационно-вычислительных систем; - основные сведения о базовых структурах данных; - основные комбинаторные и теоретико-графовые алгоритмы; - общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения; - основные криптографические протоколы системы шифрования с открытыми ключами; - криптографические средства и системы защиты информации и их программно-аппаратную реализацию; - требования к шифрам и их основные характеристики; типовые поточные и блочные шифры; - основные уязвимости программно-аппаратных компонентов информационно-телекоммуникационных систем;			

	- программно-аппаратные средства обеспечения информационной безопасности в типовых операционных систем в системах управления базами данных, вычислительных сетях; - методы анализа электрических цепей при гармонических и произвольных воздействиях; - преобразование случайных сигналов линейными и нелинейными цепями; - устройство, принцип действия и характеристики типовых линейных и нелинейных устройств; - типовые нелинейные цепи и преобразование ими радиосигналов; - спектральные и корреляционные характеристики аналоговых и дискретных детерминированных сигналов; - корреляционный и спектральный анализ случайных сигналов и помех; - основные уравнения электродинамики; - физические основы излучения и распространения радиоволн в различных средах; - особенности распространения радиоволн различных диапазонов; - математические модели сигналов, помех и каналов связи; - виды модуляции сигналов; - методы формирования и			

	преобразования сигналов в телекоммуникационных системах; - основы теории помехоустойчивости и оптимального приема; - основные принципы построения устройств квантовой и оптической электроники; - принципы построения систем на базе микропроцессоров; - современную элементную базу телекоммуникационных систем; - дискретные и цифровые сигналы и системы, основы цифровой обработки сигналов; - основы компьютерной графики; - правила выполнения и оформления электрических схем электронной техники в единой системе конструкторской документации; - средства автоматизированного проектирования устройств электронной техники; - принципы построения измерительной техники, измеряемые параметры телекоммуникационных систем; - общие принципы проектирования современных систем и сетей телекоммуникаций, включая мультисервисные сети связи; - основные этапы процесса проектирования и общие требования к содержанию проекта; - типовые модели систем и сетей телекоммуникаций,			

	применяемые при анализе, расчете и оптимизации проектируемых параметров; - уязвимости основных телекоммуникационных технологий; - технологии, средства и методы обеспечения информационной безопасности телекоммуникационных систем; - общие принципы формализации и алгоритмизации процессов функционирования устройств и систем; уметь: - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; - разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; - пользоваться нормативными документами по противодействию технической разведке; - анализировать и оценивать угрозы информационной безопасности объекта; - реализовывать и			

	контролировать выполнение требований по охране труда и технике безопасности в профессиональной деятельности; - применять основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий; - работать с современной элементной базой электронной аппаратуры; - проводить анализ показателей качества сетей и систем телекоммуникаций; - строить (выбирать) эффективные модели сигналов, помех и каналов связи, методов формирования и преобразования сигналов в телекоммуникационных системах; - осуществлять анализ помехоустойчивости и пропускной способности каналов связи; - оценивать и выбирать эффективные кодеки и модемы для телекоммуникационных систем; - разрабатывать структурные схемы систем связи с заданными характеристиками; - осуществлять удаленный доступ к базам данных; - развертывать, конфигурировать и настраивать работоспособность вычислительных систем; - реализовывать базовые алгоритмы цифровой			

	обработки сигналов; - оценивать криптографическую стойкость шифров; применять криптографические средства и системы информационной безопасности; - обеспечивать защиту от разрушающих программных воздействий; - осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации; - рассчитывать переходные процессы в линейных системах; - решать задачи по анализу и синтезу электрических цепей с использованием математических методов и вычислительной техники; - применять корреляционный и спектральный анализ сигналов; - выбирать эффективные модели сигналов, помех и каналов связи, методов формирования и преобразования сигналов в телекоммуникационных систем; - осуществлять анализ помехоустойчивости и пропускной способности каналов связи; - прогнозировать особенности распространения электромагнитных волн различных диапазонов; - использовать при проектировании различные компоненты оптических линий связи; - проводить анализ			

	логических устройств, устройств телекоммуникационных систем на базе микропроцессорной техники; - использовать стандартные методы и средства проектирования цифровых узлов и устройств; - рассчитывать цифровые фильтры различных типов и структур; - использовать типовые пакеты прикладных программ для анализа систем цифровой обработки сигналов; - применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; - применять средства автоматизированного проектирования электрических схем электронной техники; - работать с современной элементной базой электронной аппаратуры; - измерять и рассчитывать основные характеристики сигналов и помех; - пользоваться метрологическим обеспечением экспериментального исследования телекоммуникационных систем и обеспечения информационной безопасности; - разрабатывать модели и проводить статистический анализ проектируемых			

	систем и сетей телекоммуникаций; - проводить анализ показателей качества проектируемых сетей и систем телекоммуникаций; - анализировать безопасность функционирования телекоммуникационных систем; - оценивать уязвимость протоколов и интерфейсов телекоммуникационных систем; - разрабатывать политики безопасности телекоммуникационных систем; - выбирать адекватные методы моделирования и типы моделей; - разрабатывать математические модели и моделировать на ЭВМ типовые устройства телекоммуникационных систем; владеть: - профессиональной терминологией в области информационной безопасности; - навыками работы с нормативными правовыми актами; - навыками организации и обеспечения режима секретности; - методами организации и управления деятельностью служб защиты информации на предприятии; - методами и средствами технической защиты информации; - методами расчета и инструментального контроля показателей технической защищенности			

	информации; - навыками безопасного использования технических средств в профессиональной деятельности; - навыками работы с программными средствами схемотехнического моделирования; - навыками чтения принципиальных схем, построения временных диаграмм и работы узла, устройства и системы по комплекту документации; - навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений; - навыками анализа сетевых протоколов; - навыками работы с научно-технической литературой по перспективным сетям и системам связи с целью повышения эффективности защищенных телекоммуникационных систем; - навыками использования известных методов программирования и возможностей базового языка программирования для решения типовых профессиональных задач; - методами оценки криптографической стойкости алгоритмов шифрования; - криптографическими средствами и базовыми технологиями информационной безопасности;			

	- навыками защиты от разрушающих программных воздействий; - навыками рационального выбора средств и методов защиты информации объектов информатизации; - навыками анализа электрических цепей; - навыками расчета параметров элементов радиотехнических цепей; - навыками спектрального анализа сигналов; - навыками анализа преобразования сигналов в линейных и нелинейных радиотехнических цепях; - методами анализа и синтеза цифровых устройств; - методами расчета распространения радиоволн в ионосфере и тропосфере; - навыками работы с лазерами, фотоприемниками, другими оптоэлектронными устройствами; - методами анализа и синтеза цифровых устройств, микропроцессорной техники телекоммуникационных систем; - навыками цифровой обработки информации (речь, видео, данные); - навыками работы с системами автоматизированного проектирования и математического моделирования; - навыками использования графических средств представления проектных решений; - навыками оценки			

	эффективности и оптимизации параметров телекоммуникационных систем; - навыками использования современной измерительной аппаратуры при проведении измерений в телекоммуникационных системах; - методами построения и анализа моделей, применяемых в телекоммуникационных системах; - навыками составления рабочего проекта и пониманием содержания основных этапов процесса проектирования; - навыками анализа безопасности функционирования телекоммуникационных систем; - навыками работы с прикладными программами моделирования на функциональном и схемотехническом уровне иерархии моделей.			
	1. Специализация "Мониторинг в телекоммуникационных системах"**	12-17		
	2. Специализация "Системы представительской связи"	12-17		
	3. Специализация "Сети специальной связи"**	12-17		
	4. Специализация "Инструментальный контроль информационной безопасности телекоммуникационных систем"**	12-17		
	5. Специализация "Системы специальной связи и информации для органов государственной	12-17		

власти"**			
6. Специализация "Информационная безопасность космических телекоммуникационных систем" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - принципы построения систем спутниковой связи и навигации; - орбиты спутников, применяемых в системах связи и навигации; - особенности энергетики спутниковых радиолиний; - методы передачи сообщений в спутниковых системах; - отечественные и зарубежные стандарты взаимодействия космических и наземных систем; - возможности, структуру, технические характеристики бортовых и наземных командно-измерительных систем управления; - методы и средства информационной безопасности телекоммуникаций космических и наземных систем; уметь: - формулировать основные технические требования к телекоммуникационному обмены между системам космической связи и навигации; - рассчитывать основные характеристики радиолинии систем спутниковой связи и навигации;	12-17	Системы спутниковой связи и навигации Основы информационной безопасности телеуправления космическими аппаратами	ПСК-6.1 ПСК-6.2 ПСК-6.3 ПСК-6.4 ПСК-6.5

	- оценивать основные проблемы защищенного телеуправления космическими аппаратами; - определять основные параметры и структуры информационных сообщений космических систем; - оценивать реальные и предельные возможности пропускной способности, помехоустойчивости и информационной безопасности телеуправления космическими аппаратами; владеть: - терминологией в области спутниковой связи и навигации; - методами расчета зон видимости, покрытия и обслуживания систем спутниковой связи и навигации; методами и средствами защиты информации в системах космической связи и навигации; - навыками формирования команд управления космическим аппаратами и обработки телеметрической информации.			
	7. Специализация "Разработка защищенных телекоммуникационных систем" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - основы обеспечения функционирования защищенных телекоммуникационных систем в условиях	12-17	Разработка защищенных телекоммуникационных систем специального назначения Защита программных средств защищенных телекоммуникационных систем Управление информационной безопасностью	ПСК-7.1 ПСК-7.2 ПСК-7.3 ПСК-7.4 ПСК-7.5 ПСК-7.6 ПСК-7.7

	информационных конфликтов; - принципы работы основных функциональных узлов защищенных телекоммуникационных систем; - принципы работы инструментальных средств исследования программного обеспечения защищенных телекоммуникационных систем; - принципы и средства программного обеспечения защищенных телекоммуникационных систем; - основы построения систем менеджмента информационной безопасности телекоммуникаций; - основы менеджмента безопасности сетей; - основные критерии, методы и меры обеспечения доверия к информационной безопасности; - комплексную методологию обеспечения доверия к информационной безопасности защищенных телекоммуникационных систем на всех этапах их жизненного цикла; уметь: - анализировать особенности функционирования защищенных телекоммуникационных систем в условиях воздействия дестабилизирующих факторов; - разрабатывать программное обеспечение,		телекоммуникационных систем	

	реализовывать основные функциональные узлы защищенных телекоммуникационных систем на сигнальных процессорах; - применять изученные инструментальные средства для исследования программных средств защищенных телекоммуникационных систем в машинных кодах; - выявлять уязвимости защиты программных средств защищенных телекоммуникационных систем и находить пути их устранения; - проектировать и реализовывать защиту программных средств защищенных телекоммуникационных систем, исходя из поставленных целей защиты; - разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; - выбирать, разрабатывать и внедрять практические меры по управлению информационной безопасностью (от отправной точки до требуемого уровня) на основе современных международных и национальных стандартов; владеть: - навыками и приёмами расчётов основных характеристик разрабатываемых функциональных узлов защищенных			

	телекоммуникационных систем; - навыками использования базовых средств отладки аппаратного и программного обеспечения функциональных узлов защищенных телекоммуникационных систем на цифровых сигнальных процессорах; - навыками работы с современными инструментальными средствами для исследования программных средств защищенных телекоммуникационных систем; - навыками разработки защиты программных средств защищенных телекоммуникационных систем; - навыками разработки систем мониторинга информационной безопасности защищенных телекоммуникационных систем; - навыками проведения аудита информационной безопасности; - навыками применения различных методов и мер обеспечения доверия к информационной безопасности: лицензирование, аккредитация, оценка и подтверждение соответствия.			
	8. Специализация "Системы подвижной цифровой защищенной связи" С целью получения данной специализации при изучения базовой части цикла обучающийся	12-17	Основы цифровых телекоммуникационных сетей Беспроводные системы связи и их безопасность Системы позиционирования	ПСК-8.1 ПСК-8.2 ПСК-8.3 ПСК-8.4 ПСК-8.5 ПСК-8.6

	должен: знать: - историю развития беспроводных систем связи и тенденций развития систем мобильной связи и беспроводного Интернета; - основные способы разграничения пользователей в системах связи (временное, частотное, кодовое, пространственное); - основные принципы построения защищенных мобильных беспроводных систем связи; - основные характеристики стандартов широкополосного доступа; - архитектуру современных мобильных беспроводных сетей; - характеристики сигналов, используемых в современных системах мобильной беспроводной связи, а также методы их генерации, приема и обработки; - требования по обеспечению безопасности систем беспроводного доступа, современные протоколы шифрования; - принципы построения современных систем сотовой связи и беспроводного Интернета; - методы описания каналов распространения сигналов; - основные показатели качества работы беспроводных систем связи; - принципы построения современных глобальных спутниковых систем позиционирования; - принципы построения		подвижных объектов	

	современных наземных локальных и глобальных систем позиционирования в том числе в современных системах сотовой мобильной беспроводной связи и беспроводного Интернета; - характеристики сигналов используемых в глобальных и локальных системах позиционирования, основные методы их приема и обработки, источники возникновения ошибок в определении координат и скорости подвижных объектов; уметь: - рассчитывать основные характеристики приемных и передающих устройств беспроводных систем связи; - разрабатывать и реализовывать отдельные функциональные блоки приемных и передающих устройств физического уровня обработки сигналов; - рассчитывать основные показатели качества работы беспроводных систем связи; - разрабатывать и реализовывать функциональные блоки передачи, приема и обработки сигналов в системах позиционирования; - рассчитывать основные характеристики приемных и передающих систем позиционирования; - осуществлять обоснованный выбор технологий построения защищенных мобильных беспроводных систем связи			

	с учетом возможных угроз; - осуществлять построение моделей безопасности беспроводных систем связи; применять методики испытаний и оценки защищенности систем беспроводного доступа; владеть: - терминологией в области современных беспроводных систем связи; - методами расчета основных показателей качества работы беспроводных систем связи; - навыками в моделировании и оценки безопасности беспроводных систем связи; - терминологией в области глобальных и локальных систем позиционирования; - методами расчета основных показателей качества и безопасности работы систем позиционирования.			
	9. Специализация "Защита информации в радиосвязи и телерадиовещании" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - принципы построения телекоммуникационных систем и сетей различных типов; - современные и перспективные направления развития телекоммуникационных сетей и систем; - нормативную и правовую	12-17	Устройства генерирования, формирования и передачи сигналов в защищенных системах радиосвязи Устройства приема и обработки сигналов в защищенных системах радиосвязи Системы радиосвязи и сети телерадиовещания	ПСК-9.1 ПСК-9.2 ПСК-9.3 ПСК-9.4 ПСК-9.5 ПСК-9.6 ПСК-9.7 ПСК-9.8

	документацию, характерную для области технологий и систем радиосвязи и телерадиовещания; - системы, средства и методы защиты информации в сетях, системах и устройствах радиосвязи и телерадиовещания; - основы теории, методы и средства теоретического расчёта и экспериментального исследования устройств генерирования, формирования, передачи, приема и обработки сигналов в защищенных системах радиосвязи; - современную элементную базу и схемотехнику аналоговых и цифровых устройств радиосвязи и телерадиовещания; - теоретические основы и методы электромагнитной совместимости систем и устройств радиосвязи и телерадиовещания; - процедуры назначения, распределения и эффективного использования радиочастотного спектра; уметь: - формулировать основные технические требования к телекоммуникационным сетям и системам, оценивать основные проблемы, связанные с эксплуатацией и внедрением новой телекоммуникационной техники; - проводить анализ и компьютерное моделирование физических процессов в аналоговых и			

	цифровых устройствах формирования, излучения, приёма, преобразования и обработки сигналов; - оценивать реальные и предельные возможности пропускной способности, помехоустойчивости и информационной безопасности систем радиосвязи и телерадиовещания; - понимать сущность электромагнитной совместимости и процедур назначения, распределения и эффективного использования радиочастотного спектра; - организовывать и проводить испытания средств защищенной радиосвязи и телерадиовещания с целью оценки их соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов; владеть: - отечественной и международной нормативной и правовой базой в области технологий и систем радиосвязи и телерадиовещания; - методами и средствами защиты информации в сетях, системах и устройствах радиосвязи и телерадиовещания; - приёмами разработки и использования моделей телекоммуникационных сетей и систем и проверке их адекватности на практике; - методами расчёта сетей,			

	систем и устройств защищенной радиосвязи и телерадиовещания в соответствии с техническим заданием; - метрологическими принципами и навыками инструментальных измерений, используемых в области технологий и систем радиосвязи и телерадиовещания.			
	10. Специализация "Защита информации в системах связи и управления" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - особенности формирования, передачи и приема информации в системах беспроводной связи; - методы представления информации (методы кодирования, протоколы обмена) применяемые в системах беспроводной связи; - концепцию адаптивных систем обеспечения информационной безопасности инфотелекоммуникационных систем; - методы защиты от основных угроз в компьютерных сетях и телекоммуникационных системах; - методы обнаружения сетевых атак; - процессный подход к управлению информационной безопасностью;	12-17	Защита информации в системах беспроводной связи Защита информации в компьютерных сетях Планирование и управление информационной безопасностью	ПСК-10.3 ПСК-10.4 ПСК-10.5 ПСК-10.6 ПСК-10.7

	уметь: - выявлять возможные каналы перехвата информации в беспроводных системах связи и определять виды технической разведки в отношении этих каналов; и управления; - анализировать и обеспечивать безопасность распределенных автоматизированных систем; - моделировать каналы утечки информации в системах связи; - планировать процессы управления информационной безопасностью на основе современных международных и национальных стандартов; - анализировать и оценивать эффективность систем защиты информации; владеть: - методами построения беспроводных сетей; - навыками конфигурирования межсетевых экранов, виртуальных защищенных сетей и систем обнаружения атак; - навыками активного аудита; навыками разработки процедур управления информационной безопасностью; - навыками риск-анализа защищенности телекоммуникационных систем.			
	11. Специализация "Информационная безопасность	12-17	Информационная безопасность и защита	ПСК-11.1 ПСК-11.2 ПСК-11.3

	мультисервисных телекоммуникационных сетей и систем на транспорте" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - основы комплексного обеспечения информационной безопасности интегрированных телекоммуникационных и корпоративных сетей транспорта (по видам); - стандарты цифровых сетей оперативно-технологической связи и абонентского доступа, особенности и принципы организации их безопасности, методы и средства измерений и технической диагностики в защищенных сетях транспорта (по видам); уметь: - анализировать и исключать уязвимости информационной безопасности в интегрированных телекоммуникационных и корпоративных сетях, цифровых автоматических телефонных станциях, цифровой технологической связи, каналообразующих систем передачи, узлов абонентского доступа; - осуществлять рациональный выбор средств и методов защиты информации; - применять автоматизированные средства аудита и анализа защищенности сетей;		информации в интегрированных телекоммуникационных и корпоративных сетях транспорта (по видам) Специальные измерения и техническая диагностика в защищенных сетях транспорта (по видам) Цифровые сети оперативно-технологической связи и их безопасность	ПСК-11.4 ПСК-11.5

	владеть: - системным подходом к организации информационных процессов и сетевой интеграции, к анализу информационной безопасности интегрированных телекоммуникационных и корпоративных сетей; - навыками специальных измерений и технической диагностики в защищенных сетях и оценивания характеристик готовности и защищенности сетей и систем.			
	12. Специализация "Безопасность телекоммуникационных систем информационного взаимодействия" С целью получения данной специализации при изучения базовой части цикла обучающийся должен: знать: - задачи кодирования в системах информационного взаимодействия; - основные показатели качества кодеков; - методы анализа качественных показателей кодеков; - методы построения классических кодов и их декодеров; - методы турбо-кодирования; - методы моделирования кодеков; - задачи компьютерных сетей; - основные протоколы компьютерных сетей; - программно-аппаратное обеспечение	12-17	Кодирование в телекоммуникационных системах Компьютерные сети	ПСК-12.1 ПСК-12.2 ПСК-12.3 ПСК-12.4 ПСК-12.5 ПСК-12.6 ПСК-12.7 ПСК-12.8 ПСК-12.9

	компьютерных сетей; - архитектуры компьютерных сетей; уметь: - предложить способ кодирования для решения базовых задач информационного взаимодействия; - предложить эффективный метод (алгоритм) декодирования выбранного кода; - построить модель кодека и канала для экспериментальной оценки эффективности выбранного способа кодирования; - обосновать структуру сети для решения целевой задачи информационного взаимодействия; - обосновать состав и характеристики программно-аппаратного оснащения сети информационного взаимодействия; - выполнить установку и настройку основных параметров программноаппаратного обеспечения сети; - организовать автоматический сбор основных параметров программно-аппаратного обеспечения сети; - оценить главные источники уязвимостей сети; владеть: - математическим аппаратом для оценки качественных показателей кодеков; - стандартными программными средствами для моделирования кодеков и каналов передачи данных;			

	- стандартными средствами для локального и удаленного конфигурирования и управления режимами сетей информационного взаимодействия; стандартными средствами анализа эффективности информационного взаимодействия; - стандартными средствами моделирования сетей и сетевых информационных потоков.			
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	50-54		
С.4	Физическая культура	2		ОК-11 ОК-12
С.5	Учебная и производственная практики, научно-исследовательская работа (практические умения и навыки определяются ООП вуза)	18-21		ПК-5 ПК-6 ПК-9 ПК-10 ПК-12 ПК-16 ПК-31 ПК-32 ПК-33 ПК-34 ПК-35
С.6	Итоговая государственная аттестация	21-24		ОК-1 - ОК-12 ПК-1 - ПК-35 ПСК-12.1 - ПСК-12.9
	Общая трудоемкость основной образовательной программы	330		

_____

* Трудоемкость циклов С.1, С.2, С.3 и разделов С.4, С.5 включает все виды текущей и промежуточной аттестаций.

** В соответствии с п. 7.1 настоящего стандарта требования к результатам освоения и структуре ООП в части специализаций определяются вузом.

*** Суммарная трудоемкость базовых составляющих циклов С.1, С.2 и С.3 должна составлять не менее 75 процентов от общей трудоемкости указанных циклов.

Для вузов федеральных органов исполнительной власти, в которых предусмотрена военная служба и (или) служба в правоохранительных органах, нормативный срок освоения ООП может быть уменьшен за счет сокращения

продолжительности каникулярного времени обучающихся в учебном году до 45 суток, переноса части аудиторных занятий по физической культуре на часы проведения утренней зарядки и часы спортивно-массовой работы, сокращения времени, выделяемого на проведение практик путем выполнения аналогичных задач в ходе полетов, вождения боевых машин, учений, несения учебно-боевого и других дежурств, внутренней, гарнизонной, караульной и других служб и практик при условии сохранения общей трудоемкости ООП, определенной данным стандартом.

VII. Требования к условиям реализации основных образовательных программ подготовки специалиста

7.1. Образовательные учреждения самостоятельно разрабатывают и утверждают ООП подготовки специалиста, которая включает в себя учебный план, рабочие программы учебных курсов, предметов, дисциплин (модулей) и другие материалы, обеспечивающие воспитание и качество подготовки обучающихся, а также программы учебной и производственной практик, календарный учебный график и методические материалы, обеспечивающие реализацию соответствующей образовательной технологии.

Специализация ООП подготовки специалиста определяется высшим учебным заведением в соответствии с ФГОС ВПО и примерной ООП подготовки специалиста.

Требования к результатам освоения и структуре ООП подготовки специалистов в части специализаций для вузов, в которых предусмотрена военная служба и (или) служба в правоохранительных органах, определяются вузами по согласованию с федеральными органами исполнительной власти, в ведении которых находятся данные образовательные учреждения.

Реализация ООП по специальности 090302 Информационная безопасность телекоммуникационных систем допускается только при наличии у вуза лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну.

В случае, если ООП связана с освоением учебного материала, содержащего сведения, составляющие государственную тайну, то условия ее реализации должны соответствовать следующим требованиям:

наличие у лиц, участвующих в реализации образовательного процесса, содержащего сведения, составляющие государственную тайну, оформленного в установленном порядке допуска к государственной тайне по соответствующей форме;

наличие в образовательном учреждении нормативных правовых документов по обеспечению режима секретности и их выполнение;

осуществление образовательного процесса, содержащего сведения, составляющие государственную тайну, только в помещениях образовательного учреждения либо организаций, на базе которых реализуется образовательный процесс, удовлетворяющих требованиям нормативных правовых документов по режиму секретности, противодействию техническим разведкам и технической защите информации;

использование при реализации образовательного процесса, содержащего сведения, составляющие государственную тайну, средств вычислительной техники и программного обеспечения, удовлетворяющих требованиям нормативных правовых документов по режиму секретности, противодействию техническим разведкам и технической защите информации.

Высшие учебные заведения обязаны ежегодно обновлять ООП подготовки

специалиста с учетом развития науки, техники, культуры, экономики, технологий и социальной сферы.

7.2. При разработке ООП подготовки специалиста должны быть определены возможности вуза в формировании общекультурных компетенций выпускников (компетенций социального взаимодействия, самоорганизации и самоуправления, системно-деятельностного характера). Вуз обязан сформировать социокультурную среду, создать условия, необходимые для всестороннего развития личности.

Вуз обязан способствовать развитию социально-воспитательного компонента учебного процесса, включая развитие студенческого самоуправления, участие обучающихся в работе общественных организаций, спортивных и творческих клубов, научных студенческих обществ.

7.3. Реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций, психологические и иные тренинги) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся. В рамках учебных курсов, связанных с проблемами обеспечения информационной безопасности, должны быть предусмотрены встречи с представителями органов государственной власти и управления, российских компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ООП подготовки специалиста, особенностью контингента обучающихся и содержанием конкретных дисциплин. В целом в учебном процессе они должны составлять не менее 25 процентов аудиторных занятий, в том числе специальных профессиональных деловых игр (комплексных учений) в объеме не менее одной недели. Занятия лекционного типа для соответствующих групп обучающихся не могут составлять более 55 процентов аудиторных занятий.

7.4. В учебной программе каждой дисциплины (модуля) должны быть четко сформулированы конечные результаты обучения в органичной увязке с осваиваемыми знаниями, умениями и приобретаемыми компетенциями в целом по ООП подготовки специалиста.

Общая трудоемкость дисциплины не может быть менее двух зачетных единиц (за исключением дисциплин по выбору обучающихся и факультативных дисциплин). По дисциплинам, трудоемкость которых составляет более трех зачетных единиц, должна выставляться оценка ("отлично", "хорошо", "удовлетворительно", "неудовлетворительно").

7.5. ООП подготовки специалиста должна содержать дисциплины по выбору обучающихся в объеме не менее одной трети вариативной части суммарно по циклам С.1, С.2 и С.3. Порядок формирования дисциплин по выбору обучающихся устанавливает ученый совет вуза.

7.6. Максимальный объем учебной нагрузки обучающихся не может составлять более 54 академических часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы по освоению ООП и факультативных дисциплин, устанавливаемых вузом дополнительно к ООП подготовки специалиста и необязательными для изучения обучающимися.

Объем факультативных дисциплин не должен превышать 13 зачетных единиц за весь период обучения.

7.7. Объем аудиторных учебных занятий в неделю при освоении ООП в очной форме обучения составляет не менее 27 и не более 36 академических часов. В указанный объем не входят обязательные аудиторные занятия по физической

культуре.

7.8. В случае реализации ООП подготовки специалиста в иных формах обучения максимальный объем аудиторных занятий устанавливается в соответствии с Типовым положением об образовательном учреждении высшего профессионального образования (высшем учебном заведении), утвержденным постановлением Правительства Российской Федерации N 71 от 14 февраля 2008 г. (Собрание законодательства Российской Федерации, 2008, N 8, ст. 731).

7.9. Общий объем каникулярного времени в учебном году должен составлять 7-10 недель, в том числе не менее двух недель в зимний период.

В высших учебных заведениях, в которых предусмотрена военная служба и (или) служба в правоохранительных органах, продолжительность каникулярного времени обучающихся определяется в соответствии с нормативными правовыми актами, регламентирующими порядок прохождения службы**.

7.10. Раздел "Физическая культура" ("Физическая подготовка" - для вузов, в которых предусмотрена военная служба и (или) служба в правоохранительных органах) трудоемкостью две зачетные единицы реализуется: при очной форме обучения, как правило, в объеме 400 часов, при этом объем практической, в том числе игровых видов, подготовки должен составлять не менее 360 часов.

7.11. Вуз обязан обеспечить обучающимся реальную возможность участвовать в формировании своей программы обучения, включая возможную разработку индивидуальных образовательных программ.

7.12. Вуз обязан ознакомить обучающихся с их правами и обязанностями при формировании ООП подготовки специалиста, разъяснить, что избранные обучающимися дисциплины (модули) становятся для них обязательными.

7.13. ООП подготовки специалиста вуза должна включать лабораторные практикумы и практические занятия по дисциплинам (модулям) базовой части циклов С.2 и С.3, формирующим у обучающихся умения и навыки в области физики, информатики, языков программирования, безопасности жизнедеятельности, электроники и схемотехники, теории радиотехнических сигналов, теории электрических цепей, теории электрической связи, сетей и систем передачи информации, цифровой обработки сигналов, технической защиты информации, программно-аппаратным средствам обеспечения информационной безопасности, измерениям в телекоммуникационных системах, а также по дисциплинам специализации и вариативной части, рабочие программы которых предусматривают цели формирования у обучающихся соответствующих умений и навыков.

7.14. Наряду с установленными законодательными и другими нормативными правовыми актами, правами и обязанностями обучающиеся имеют следующие права и обязанности:

обучающиеся имеют право в пределах объема учебного времени, отведенного на освоение дисциплин (модулей) по выбору, предусмотренных ООП подготовки специалиста, выбирать конкретные дисциплины (модули);

при формировании своей индивидуальной образовательной программы обучающиеся имеют право получить консультацию в вузе по выбору дисциплин (модулей) и их влиянию на будущую специализацию ООП подготовки специалиста;

обучающиеся при переводе из другого высшего учебного заведения при наличии соответствующих документов имеют право на перезачет освоенных ранее дисциплин (модулей) на основании аттестации;

обучающиеся обязаны выполнять в установленные сроки все задания, предусмотренные ООП подготовки специалиста.

7.15. Раздел ООП подготовки специалиста "Учебная и производственная

практики, научно-исследовательская работа" является обязательным и представляет собой форму организации учебного процесса, непосредственно ориентированных на профессионально-практическую подготовку обучающихся.

Конкретные виды практик определяются ООП вуза. Цели и задачи, программы и формы отчетности определяются вузом по каждому виду практики.

Практики проводятся в сторонних организациях, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации) или на кафедрах и в лабораториях вуза (учебная практика), обладающих необходимым кадровым и научно-техническим потенциалом.

В высших учебных заведениях, в которых предусмотрена военная служба и (или) служба в правоохранительных органах за счет времени, выделяемого на практики, могут проводиться специальные профессиональные деловые игры (комплексные учения).

Аттестация по итогам практики проводится на основании оформленного в соответствии с установленными требованиями письменного отчета и отзыва руководителя практики от организации. По итогам аттестации выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно).

7.16. Научно-исследовательская работа является обязательным разделом основной образовательной программы подготовки специалиста. Она направлена на комплексное формирование общекультурных, профессиональных и профессионально-специализированных компетенций в соответствии с требованиями ФГОС ВПО.

При разработке программы научно-исследовательской работы высшее учебное заведение должно предоставить возможность обучающимся:

изучать специальную литературу и другую научно-техническую информацию о достижениях отечественной и зарубежной науки и техники в соответствующей области знаний;

участвовать в проведении научных исследований или выполнении технических разработок;

осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме (заданию);

принимать участие в стендовых и промышленных испытаниях опытных образцов (партий) проектируемых изделий;

составлять отчеты (разделы отчета) по теме или ее разделу (этапу, заданию), готовить рефераты;

выступить с докладом на конференции, научном семинаре.

В процессе выполнения научно-исследовательской работы и оценки ее результатов должно проводиться широкое обсуждение в учебных структурах вуза с привлечением работодателей, позволяющее оценить уровень компетенций, сформированных у обучающихся. Необходимо также дать оценку компетенций, связанных с формированием профессионального мировоззрения и определения уровня культуры.

7.17. Реализация ООП подготовки специалиста должна обеспечиваться научно-педагогическими кадрами, имеющими, как правило, базовое образование, соответствующее профилю преподаваемой дисциплины, и систематически занимающимися научной и (или) научно-методической деятельностью.

Доля преподавателей, имеющих ученую степень и (или) ученое звание, в общем числе преподавателей, обеспечивающих образовательный процесс по данной ООП, должна быть не менее 65 процентов, ученую степень доктора наук (в том числе степень, присваиваемую за рубежом, документы о присвоении которой прошли

установленную процедуру признания и установления эквивалентности) и (или) ученое звание профессора должны иметь не менее 9 процентов преподавателей.

Преподаватели профессионального цикла должны иметь базовое образование и (или) ученую степень, соответствующие профилю преподаваемой дисциплины, или опыт деятельности в сфере обеспечения информационной безопасности.

Не менее 70 процентов преподавателей (в приведенных к целочисленным значениям ставок), обеспечивающих учебный процесс по профессиональному циклу, должны иметь ученые степени или ученые звания, при этом ученые степени доктора наук или ученое звание профессора должны иметь не менее 11 процентов преподавателей.

К образовательному процессу должно быть привлечено не менее пяти процентов преподавателей из числа действующих руководителей и работников профильных организаций, предприятий и учреждений.

До 10 процентов от общего числа преподавателей, имеющих ученую степень и (или) ученое звание может быть заменено преподавателями, имеющими стаж практической работы по данному направлению на должностях руководителей или ведущих специалистов не менее 5 последних лет.

В вузах, в которых предусмотрена военная служба и (или) служба в правоохранительных органах к преподавателям с учеными степенями и (или) учеными званиями приравниваются преподаватели военно-(специальных) профессиональных дисциплин, не имеющие ученых степеней и ученых званий, имеющие профильное высшее образование, опыт работы в войсках (на флотах), штабах, правоохранительных органах, учреждениях не менее 10 лет, воинское звание не ниже "подполковник", а также или боевой опыт, или государственные награды, или государственные (отраслевые) почетные звания, или государственные премии. В числе преподавателей с ученой степенью доктора наук и (или) ученым званием профессора могут учитываться преподаватели военно-(специальных) профессиональных учебных дисциплин с ученой степенью кандидата наук, имеющие или государственные награды, или государственные (отраслевые) почетные звания, или государственные премии.

В структуре вуза, реализующего данную основную образовательную программу подготовки специалиста, должна быть отдельная выпускающая кафедра по специальности "Информационная безопасность телекоммуникационных систем".

Общее руководство содержанием теоретической и практической подготовки по специализации должно осуществляться штатным научно-педагогическим работником вуза, имеющим ученую степень доктора или кандидата наук и (или) ученое звание профессора или доцента, стаж работы в образовательных учреждениях высшего профессионального образования не менее трех лет. К общему руководству содержанием теоретической и практической подготовки по специализации может быть привлечен высококвалифицированный специалист в соответствующей сфере профессиональной деятельности.

7.18. ООП подготовки специалиста должна обеспечиваться учебно-методической документацией и материалами по всем учебным курсам, дисциплинам (модулям) ООП. Содержание каждой из таких учебных дисциплин (модулей) должно быть представлено в сети Интернет или локальной сети образовательного учреждения с выполнением установленных требований по защите информации.

Внеаудиторная работа обучающихся должна сопровождаться методическим обеспечением и обоснованием времени, затрачиваемого на ее выполнение.

Каждый обучающийся должен быть обеспечен доступом к электронно-библиотечной системе, содержащей издания по основным изучаемым дисциплинам и сформированной на основании прямых договоров с правообладателями учебной и

учебно-методической литературы.

При этом должна быть обеспечена возможность осуществления одновременного индивидуального доступа к такой системе не менее чем для 25 процентов обучающихся.

Библиотечный фонд должен быть укомплектован печатными и (или) электронными изданиями основной учебной литературы по дисциплинам базовой части всех циклов, изданными за последние 10 лет (для дисциплин базовой части гуманитарного, социального и экономического цикла - за последние пять лет), из расчета не менее 25 экземпляров таких изданий на каждые 100 обучающихся.

Фонд дополнительной литературы помимо учебной должен включать официальные, справочно-библиографические и специализированные периодические издания, в том числе, правовые нормативные акты и нормативные методические документы в области информационной безопасности в расчете один-два экземпляра на каждые 100 обучающихся.

Электронно-библиотечная система должна обеспечивать возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет с выполнением установленных требований по защите информации.

Оперативный обмен информацией с отечественными и зарубежными вузами и организациями должен осуществляться с соблюдением требований законодательства Российской Федерации об интеллектуальной собственности и защиты сведений, составляющих государственную тайну, а также международных договоров Российской Федерации в области интеллектуальной собственности. Для обучающихся должен быть обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам в том числе, по тематике информационной безопасности.

Каждому обучающемуся должен быть обеспечен доступ к комплектам библиотечного фонда, состоящего не менее чем из пяти наименований отечественных и не менее четырех наименований зарубежных журналов.

7.19. Ученый совет высшего учебного заведения при введении ООП подготовки специалиста утверждает размер средств на реализацию соответствующих ООП.

Финансирование реализации ООП подготовки специалиста должно осуществляться в объеме не ниже установленных нормативов финансирования высшего учебного заведения***.

7.20. Высшее учебное заведение, реализующее ООП подготовки специалистов, должно располагать материально-технической базой, включая приборы, оборудование и программно-аппаратные средства специального назначения, обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, практической и научно-исследовательской работы обучающихся, предусмотренных учебным планом вуза и соответствующей действующим санитарным и противопожарным правилам и нормам.

Минимально необходимый для реализации ООП подготовки специалистов перечень материально-технического обеспечения включает в себя:

лаборатории в области:

- физики;
- электроники и схемотехники;
- сетей и систем передачи информации;
- технической защиты информации;
- измерений в телекоммуникационных системах;
- программно-аппаратных средств обеспечения информационной безопасности.

Лаборатории высшего учебного заведения должны быть оснащены современным оборудованием, стендами, приборами, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой ООП.

Специально оборудованные кабинеты и аудитории в области:

иностранного языка;

информатики;

интернет-технологий;

сетевых технологий;

цифровой обработки сигналов.

Лаборатории и специально оборудованные кабинеты и аудитории должны быть предусмотрены также для реализации дисциплин (модулей) специализации и вариативной части, рабочие программы которых предусматривают цели формирования у обучающихся соответствующих умений и навыков.

Компьютерные классы должны быть оборудованы современной вычислительной техникой для занятий по дисциплинам из расчета одно рабочее место на одного обучаемого при проведении занятий в данных классах.

При использовании электронных изданий и проведении самостоятельной подготовки вуз должен обеспечить обучающихся возможностью выхода в сеть Интернет из расчета не менее одного рабочего места на 10 обучающихся по данной ООП.

Вуз должен быть обеспечен необходимым комплектом лицензионного программного обеспечения и сертифицированными программными и аппаратными средствами защиты информации.

VIII. Требования к оценке качества освоения основных образовательных программ подготовки специалиста

8.1. Высшее учебное заведение обязано обеспечивать гарантию качества подготовки, в том числе путем:

разработки стратегии по обеспечению качества подготовки выпускников с привлечением представителей работодателей;

мониторинга, периодического рецензирования образовательных программ;

разработки объективных процедур оценки уровня знаний и умений обучающихся, компетенций выпускников;

обеспечения компетентности преподавательского состава;

регулярного проведения самообследования по согласованным критериям для оценки деятельности (стратегии) и сопоставления с другими образовательными учреждениями с привлечением представителей работодателей;

информирования общественности о результатах своей деятельности, планах, инновациях.

8.2. Оценка качества освоения основных образовательных программ подготовки специалиста должна включать текущий контроль успеваемости, промежуточную аттестацию обучающихся и итоговую государственную аттестацию выпускников.

8.3. Конкретные формы и процедуры текущего и промежуточного контроля знаний по каждой дисциплине разрабатываются вузом самостоятельно и доводятся до сведения обучающихся в течение первого месяца от начала обучения по конкретной дисциплине.

8.4. Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей ООП подготовки специалиста (текущий

контроль успеваемости и промежуточная аттестация) создаются фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить знания, умения и уровень сформированности компетенций. Фонды оценочных средств разрабатываются и утверждаются вузом.

Фонды оценочных средств должны быть полными и адекватными отображениями требований ФГОС ВПО по данному направлению подготовки (специальности), соответствовать целям и задачам конкретной ООП подготовки специалиста и её учебному плану. Они призваны обеспечивать оценку качества общекультурных, профессиональных и профессионально-специализированных компетенций, приобретаемых выпускником в соответствии с этими требованиями.

При разработке оценочных средств для контроля качества изучения модулей, дисциплин, практик должны учитываться все виды связей между включенными в них знаниями, умениями, навыками, позволяющие установить качество сформированных у обучающихся компетенций и степень общей готовности выпускников к профессиональной деятельности.

Вузом должны быть созданы условия для максимального приближения системы контроля качества освоения обучающимися ООП к условиям их будущей профессиональной деятельности. С этой целью, кроме преподавателей конкретной дисциплины, в качестве внешних экспертов должны активно привлекаться работодатели (представители заинтересованных организаций), преподаватели, читающие смежные дисциплины.

8.5. Обучающимся, должна быть предоставлена возможность оценивания содержания, организации и качества учебного процесса в целом, а также работы отдельных преподавателей.

8.6. Итоговая государственная аттестация направлена на установление соответствия уровня профессиональной подготовки выпускников требованиям ФГОС ВПО.

Итоговая государственная аттестация включает защиту выпускной квалификационной работы (дипломного проекта, дипломной работы). Государственный экзамен вводится по решению ученого совета вуза.

Требования к содержанию, объему и структуре выпускной квалификационной работы, а также требования к государственному экзамену (при наличии) определяются вузом.

---

* Одна зачетная единица соответствует 36 академическим часам.

** Статья 30 Положения о порядке прохождения военной службы, утвержденного Указом Президента Российской Федерации от 16 сентября 1999 г. N 1237 "Вопросы прохождения военной службы" (Собрание законодательства Российской Федерации, 1999, N 38, ст. 4534).

*** Пункт 2 статьи 41 Закона Российской Федерации "Об образовании" от 10 июля 1992 г. N 3266-1 (Собрание законодательства Российской Федерации, 1996, N 3, ст. 150; 2002, N 26, ст. 2517; 2004, N 30, ст. 3086; N 35, ст. 3607; 2005, N 1, ст. 25; 2007, N 17, ст. 1932; N 44, ст. 5280).